LA-UR-21-25301
Approved for public release; distribution is unlimited.

Title: FLC Award: QED: Quantum Ensured Defense of the Smart Electric Grid

Author(s): Stern, Ariana Kayla

Intended for: Report

Issued: 2021-06-04

FLC Award: QED: Quantum Ensured Defense of the Smart Electric Grid

1. Please explain your technology, the problem it solves and its benefits.

A reliable electric power supply is crucial for modern day life as well as national security, economic productivity, and life-and-death essentials. During the COVID pandemic, internet and cell communications became a “must-have” for government and business operations, education, and communicating COVID testing for vaccine information. Loss of electric power quickly leads to human health and national security emergencies. When a major winter storm hit Texas in mid-February 2021, the system was overwhelmed and over 4M people lost power. Although this crisis arose from an unprecedented weather event – not a cyberattack – it serves as a vivid illustration of the impact power disruption can have on our American way of life. The recent cyberattack on the Colonial Oil Pipeline also provides a stark reminder that infrastructure supporting our daily lives has vulnerabilities.

Scientists in the field of cryptography have developed highly complex, mathematically based security code problems to protect these critical infrastructure operations. These computer codes bordered on the edge of being unbreakable because they were built upon very difficult mathematical problems. It is a credit to current day cryptographers that the nation’s grid has remained so secure. But new approaches to computer such as quantum threaten to make current cryptography potentially breakable. As computing power steadily increases, so does the chance that adversaries will decode these complex encryptions. Current encryption systems rely on computational difficulty, such as factoring a large number, for defense against eavesdropping, impersonation, or other types of malicious action. Future advances in computing power, efficient algorithms, and artificial intelligence have the potential to erode the security of current encryption systems. This concern is particularly relevant to critical infrastructure, such as electrical grids, which cannot be quickly updated or patched to accommodate every new security vulnerability.

Scientists at Los Alamos National Laboratory are seeking to escape this ongoing attack-defend cycle by developing a new method for protecting information called Quantum Ensured Defense (QED). Instead of mathematical complexity, this method uses physics: the unusual behavior of the quantum realm. Single particles of light, or photons, are used to create cryptographic “keys” which can be used to “lock” control signals into secret codes.

The objectives for QED is to use quantum communications to authenticate control systems data with low latency, operate securely in networked topology, and engineer designs suitable for large-scale deployment. Latency (any extra delay added by the security system) is a crucial performance metric for grid communications. Any electrical disturbance on the grid travels very quickly: control signals must also travel and be used quickly or else they are simply too late to matter. For this reason, grid controls signals cannot tolerate significant latency; typically no more than a few milliseconds.

Currently, information that is sent through the internet is passed through the optical fibers as pulses of photons from a transmitter on one end to a receiver at the other. QED uses these same principles and goes further by exploiting the unusual behavior of the quantum realm. By making the light pulses so dim that they contain on average a photon, we change from “classical” physics, familiar in our everyday lives, to the unfamiliar rules of quantum physics. Quantum transmitter and receiver devices, designed at Los Alamos, are placed in power plants or substations to establish secure links. They encode information onto individual photons at the transmitter, send the photons over optical fibers, then detect the photons and recover the information at the receiver. We know the information is protected for three reasons: a photon cannot be cut in half; a photon cannot be accurately copied; and a photon cannot even be measured without changing it in some way.

Los Alamos and Oak Ridge national labs with the Electric Power Board of Chattanooga (EPB) successfully demonstrated the integrated quantum communication system on a commercial metro scale system. Together they performed field demonstrations of a quantum trusted node network, comprised of three different Quantum Key Distributions systems (QKD), on EPB's optical fiber network that included their communications center and substations. The field tests successfully demonstrated the interoperability of these diverse QKD systems' keys and validated the generation and distribution of network for use in critical infrastructure focused applications. This made quantum science and optical physics compatible with existing utility systems and software programs, preparing it for deployment across the field.

QED has the following benefits:

- Establishes resilient networks using existing architectures
- Provides plug and play ease of use
- Meets latency requirements
- Physical-layer authentication protects the grid from spoofing and impersonation
- Provides immediate notification if tampering or disruption is detected
- Makes these systems immune to any attack that is theoretically possible

2. Who/what are or will be the markets or consumer of this technology?

The average age of the United States electrical grid systems is forty years, with over 25% of the grid being fifty years old or older. This antiquated electric grid is also undergoing unprecedented changes with widespread adoption of renewable energy sources, a fast-growing fleet of electric vehicles, and ever-increasing pressure for efficiency. For these reasons and more, the control of the information and power flowing through the grid is essential for U.S. growth and prosperity. The current work has focused on protecting the electrical grid although many of the technologies we've developed could be adapted to protect other types of infrastructure under computer control that is subject to hacking.

3. What partnerships, if any, formed to help develop and potentially transfer the technology?

The Department of Energy's Office of Electricity funded both Los Alamos and Oak Ridge through an Inter-Entity Work Order (IEWO) from 2017-2020. Together with EPB they have created a communication system for the electric grid that is secure and infallible. QED for the Smart Electric Grid is a giant leap forward in electric grid communications security. Los Alamos has spearheaded joint demonstrations with Oak Ridge, EPB (power utility in Chattanooga, TN), and Qubitekk Inc. to show seamless interoperability of disparate quantum communication systems. As part of the partnership QED is running on EPB's metro scale commercial lines. Together the team is working to overcome existing distance limitations by linking systems through trusted nodes which are not contingent on physical security of the node.

4. What patents were filed or planned to be filed?

The Quantum-Secured Communications Overlay for Optical Fiber Communications Networks patent was issued on May 14, 2019. In the near future Los Alamos will be posting a commercial call seeking a collaboration partner to participate in a Cooperative Research and Development Agreement (CRADA) to further develop this technology for its unique applications. Ideally, the collaboration will lead to additional IP being generated.

U.S. Pat. No. 10,291,399 entitled “Quantum-Secured Communications Overlay for Optical Fiber Communications Networks” issued on May 14, 2019. (S133099).

Figure 1 Claira Safi, Lead Engineer on QED, works on a Quantum Hardware Security Module

Figure 2 Top view of QED receiver, showing Control Logic & Computer board, polarization modulators, and photon detector modules.

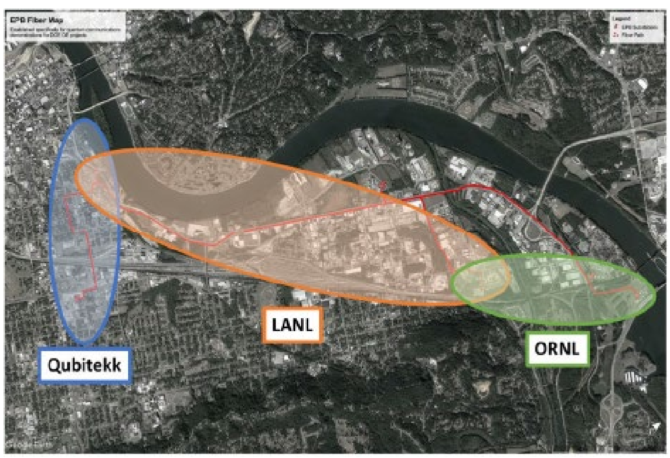

Figure 3 Back-to-back operation of three quantum communication systems, each operating on different physical principles during the successful field demonstration with Oak Ridge National Lab, Qubitekk Inc., and EPB in Chattanooga, Tennessee. Red line indicates layout of optical fibers on EPB's metroscale commercial system.

Video link: https://youtu.be/zli5meiHT74